10 USCS § 2224 (2000)

§ **2224.** Defense Information Assurance Program

(a) Defense Information Assurance Program. The Secretary of Defense shall carry out a program, to be known as the "Defense Information Assurance Program", to protect and defend Department of Defense information, information systems, and information networks that are critical to the Department and the armed forces during day-to-day operations and operations in times of crisis.

(b) Objectives of the program. The objectives of the program shall be to provide continuously for the availability, integrity, authentication, confidentiality, nonrepudiation, and rapid restitution of information and information systems that are essential elements of the Defense Information Infrastructure.

(c) Program strategy. In carrying out the program, the Secretary shall develop a program strategy that encompasses those actions necessary to assure the readiness, reliability, continuity, and integrity of Defense information systems, networks, and infrastructure. The program strategy shall include the following:

(1) A vulnerability and threat assessment of elements of the defense and supporting nondefense information infrastructures that are essential to the operations of the Department and the armed forces.

(2) Development of essential information assurances technologies and programs.

(3) Organization of the Department, the armed forces, and supporting activities to defend against information warfare.

(4) Joint activities of the Department with other departments and agencies of the Government, State and local agencies, and elements of the national information infrastructure.

(5) The conduct of exercises, war games, simulations, experiments, and other activities designed to prepare the Department to respond to information warfare threats.

(6) Development of proposed legislation that the Secretary considers necessary for implementing the program or for otherwise responding to the information warfare threat.

(d) Coordination. In carrying out the program, the Secretary shall coordinate, as appropriate, with the head of any relevant Federal agency and with representatives of those national critical information infrastructure systems that are essential to the operations of the Department and the armed forces on information assurance measures necessary to the protection of these systems.

(e) Annual report. Each year, at or about the time the President submits the annual budget for the next fiscal year pursuant to section 1105 of title 31, the Secretary shall submit to Congress a report on the Defense Information Assurance Program. Each report shall include the following:

(1) Progress in achieving the objectives of the program.

(2) A summary of the program strategy and any changes in that strategy.

(3) A description of the information assurance activities of the Office of the Secretary of Defense, Joint Staff, unified and specified commands, Defense Agencies, military departments, and other supporting activities of the Department of Defense.

(4) Program and budget requirements for the program for the past fiscal year, current fiscal year, budget year, and each succeeding fiscal year in the remainder of the current future-years defense program.

(5) An identification of critical deficiencies and shortfalls in the program.

(6) Legislative proposals that would enhance the capability of the Department to execute the program.

(f) Information assurance test bed. The Secretary shall develop an information assurance test bed within the Department of Defense to provide--

(1) an integrated organization structure to plan and facilitate the conduct of simulations, war games, exercises, experiments, and other activities to prepare and inform the Department regarding information warfare threats; and

(2) organization and planning means for the conduct by the Department of the integrated or joint exercises and experiments with elements of the national information systems infrastructure and other non-Department of Defense organizations that are responsible for the oversight and management of critical information systems and infrastructures on which the Department, the armed forces, and supporting activities depend for the conduct of daily operations and operations during crisis.

HISTORY:

(Added Oct. 5, 1999, P.L. 106-65, Div A, Title X, Subtitle E, § 1043(a), 113 Stat. 760.)